REMARKS

Claims 1-5, 8-11, 16-18, 24, 38-40, 47, and 61 are currently pending in the present application, with Claims 16, 17, 38, 39, and 61 being amended. Reconsideration and reexamination of the claims as amended and added are respectfully requested.

The Examiner objected to Claim 61 for reasons of formality. Applicants have amended Claim 61 and respectfully submit that Claim 61 complies with all formal requirements.

The Examiner rejected Claims 16-18, 24, 38-40, and 47 under 35 U.S.C. § 102(e) as being anticipated by Kuroda et al. (U.S. patent no. 6,915,434). This rejection is respectfully traversed.

As previously communicated and repeated here for the convenience of the Examiner, the present invention is directed to a scalable secured communication network that facilitates communications to and between a group of authorized users within the network. A preferred embodiment of the present invention is shown in Figure 1 of the present application, wherein each of the authorized user (shown as communication interfaces 101) possess a unique seed (small letters a-h) that are unique to the particular communication interface for generating keys to decrypt and/or encrypt messages between the particular communication interface and the master station 107. As also shown in Figure 1, all of the communication interfaces also possess a common seed "B" that can be used to generate keys for decrypting messages received from the master station 107 that are intended to be received by everyone within the secured communication network. For instance, if the secured network is a satellite premium TV subscription service, then each of the users may use common seed "B" to generate decryption keys for decrypting regular satellite programming signal.

With specific respect to amended Claims 16 and 38, the claimed inventions are directed to a method (and a computer software for performing the method) by which a signal is

received and detected to be either a unicast or a multicast signal (e.g., either a message intended for an individual receiver or multiple receivers). If the message received is detected to be a unicast transmission, then a unique cryptographic key generated from the unique seed (e.g., keys a-h as shown in Fig. 1) is used to encrypt or decrypt the message; if the message received is detected to be a multicast transmission, then a common cryptographic key generated from the common seed is used (note that if the signal is detected to be a broadcast signal (e.g., public information), then no cryptographic keys would be needed). The invention claimed by Claims 16 and 38 essentially provides a two-tiered cryptographic communication method that allows individual users to have the flexibility in transmitting/receiving messages with other individual users, or with the group as a whole, while at the same time avoiding any necessity for centralized key distribution for each of the message sessions.

Kuroda does not contain any disclosure or suggestion of a cryptographic communication method in which a received signal is detected to be a particular type of signal, such as a unicast signal or a multicast signal. Nor does Kuroda contain any disclosure or suggestion or selecting different types of cryptographic keys dependent on whether the received signal is detected to be a unicast signal or a multicast signal.

Rather, Kuroda is directed to a hierarchical storage facility wherein individual storage apparatuses have unique individual cryptographic keys and a common cryptographic key (see Abstract). The individual cryptographic keys are used only when electronic data is to be stored within the individual storage apparatuses, whereas the common key is used only when the electronic data is being transported between the storage apparatuses (see col. 5, lines 25-32).

No teachings or suggestions are made as to distinguishing the characteristics of the received messages, or selecting the type of cryptographic keys depending on the characteristic of the received messages.

The Examiner points to col. 9, lines 43-59 and col. 10, lines 7-17 of Kuroda as teachings of generating different types of cryptographic keys. Applicants respectfully disagree. Applicants respectfully submit that the cited portions of Kuroda simply discuss distribution of individual keys by the master key storage unit. Specifically, as shown in Fig. 12 of Kuroda, upon receiving instruction for generating an individual key for an individual storage apparatus, a master key is obtained from the master key storage unit to generate an individual key for that individual unit; this is essentially a part of the set up processes. Fig. 13 shows a similar set up process for generating a group key. No mention whatsoever is made as to determining the characteristics of a message received and selecting the appropriate key in response to that determination. Accordingly, Applicants respectfully submit that Claims 16-18, 24, 38-40, and 47 are not anticipated by Kuroda.

The Examiner rejected Claim 61 under 35 U.S.C. § 102(e) as being anticipated by Wright et al. (U.S. patent no. 6,084,969).[1] This rejection is respectfully traversed.

Claim 61 is directed to a method of relaying unicast communication between individual users of a user group. Specifically, as recited in Claim 61, each of the communication interface is equipped with a cryptographic key generator for generating a key from a seed value that is unique to the communication interface. Importantly, the corresponding seed values for all of the communication interfaces are also stored at a master station, which, upon receiving an encrypted transmission from a communication interface, looks up the identification of the

communication interface to retrieve a corresponding seed value and generates a corresponding cryptographic key from the seed value to decrypt the message. If the message was intended for another one of the communication interface, the master station then looks up the seed value of the intended recipient and generates a cryptographic key for re-encrypting the message prior to sending the message to the recipient. An important advantage of the claimed invention is that the cryptographic keys are always generated in situ (at location), avoiding the necessity to transmit the keys. By avoiding having to transmit the keys, the security of the encryption system is enhanced since an eavesdropper will not have any opportunity to intercept the cryptographic key.

Wright does not contain any disclosure of generating, in situ, the cryptographic keys at both the sender and the receiver end of a transmission. Rather, Wright teaches a pager system wherein each of the pager has a unique public key, which is stored in a look up table at the proxy server. Specifically, Wright teaches generating, at the pager, a session key for each transmission by the pager. Since the session keys are generated at the pager and unknown to the proxy server, the generated session keys are first encrypted via the pager's public key and transmitted to the proxy server, which decrypts the session key with the pager public key. Once the key distribution by the pager to the proxy server is established, the pager then transmits messages to the proxy server using the session key. The present invention as claimed in Claim 61 is distinguishable from Wright in that the claimed invention does NOT involve any key distribution between the communication devices. Rather, the master station

[1] In the Detailed Action, the Examiner stated that "Claim 63" is rejection. Applicants believe this was an error and that

generates, in situ, each of the session keys being used by the communication interfaces by using the seed value of the communication interfaces that are stored at the master station. Wright simply does not teach storing a seed value at both the communication interface and the master station for generating symmetrical keys to be used for encryption. Rather, the session keys generated by the pagers are first transmitted to the proxy server. The necessity of transmitting the session key is a weakness in Wright's system in that an eavesdropper can intercept and decipher the session key being transmitted by the pager. The present invention overcomes this disadvantage by avoiding the necessity of key distribution. Accordingly, Applicants respectfully submit that Claim 61 is not anticipated by, or obvious in view of, Wright.

The Examiner rejected Claims 17 and 39 under 35 U.S.C. § 103(a) as being unpatentable over Kuroda in view of Jones (U.S. patent no. 5,412,730). This rejection is respectfully traversed. Kuroda does not contain any disclosure or suggestion of a cryptographic communication method in which a received signal is detected to be a particular type of signal, such as a unicast signal or a multicast signal. Nor does Kuroda contain any disclosure or suggestion or selecting different types of cryptographic keys dependent on whether the received signal is detected to be a unicast signal or a multicast signal. Jones fails to make up the deficiencies of Kuroda. Rather, Jones is simply directed to a encryption system in which transmitter and receiver both have pseudo-random generators for generating symmetrical encryption keys. Even when combined, the references do not teach or suggest the invention

---

the Examiner intended to reject Claim 61.

recited by dependent Claims 17 and 39. Accordingly, Applicants respectfully submit that Claims 17 and 39 are not obvious of Kuroda and Jones.

In view of the above, each of the presently pending claims in this application is believed to be in immediate condition for allowance. If it is determined that a telephone conversation would expedite the prosecution of this application, the Examiner is invited to telephone the undersigned at the number given below.

In the unlikely event that the transmittal letter is separated from this document and the Patent Office determines that an extension and/or other relief is required, applicant petitions for any required relief including extensions of time and authorizes the Assistant Commissioner to charge the cost of such petitions and/or other fees due in connection with the filing of this document to **Deposit Account No. 03-1952** referencing docket no. 578062000100. However, the Assistant Commissioner is not authorized to charge the cost of the issue fee to the Deposit Account.

Dated: January 26, 2006

Respectfully submitted,

By _____
David T. Yang
Registration No.: 44,415
MORRISON & FOERSTER LLP
555 W. Fifth Street, Suite 3500
Los Angeles, CA 90013
(213) 892-5587
Attorneys for Applicant